รายการอ้างอิง

[1] Foster, I., Kesselman, C., Tsudik, G., Tuecke, S. *In proceeding of 5th ACM Conference on Computer and Communications Security Conference*, 1998, pp. 83-92.

[2] Foster, I., Kesselman, C., and Tuecke, S. "Anatomy of the Grid: Enabling Scalable Virtual Organizations", *International J. Supercomputer Applications,*15(3) 2001, pp.115-128.

[3] German, C., Steve, M., Tim, F., Francesco, G., Wolfgang, H., Dave, K., Brian, L. "The DataGrid Architecture" July 2, 2001.

[4] Hitchens, M., and Varadharajan, V. "Tower: A Language for Role Based Access Control", *Lecture Notes in Computer Science v. 1358*, 1995.

[5] Melati, D., Yin, M., Theng, Y., Hoe-Lian, D., and Lim, E. "Towards a Role-Based Metadata Scheme for Educational Digital Libraries". August 18, 2003.

[6] Sandhu, S., Coyne, J., Feinstein, L., and Youman, E. "Role-Base Access Control Models", *In proceeding of 9th IEEE Computer Security Foundations Workshop*, Dromquinna Manor, Kenmare, County Kerry, Ireland, 1996, pp. 38-47

[7] Wahl, M., Howes, T., and Kille, S. "Lightweight directory access protocol (v3)", *RFC 2251, Internet Engineering Task Force*, 1997.

[8] Active Directory Architecture, Available from: http://www.microsoft.com .

[9] MDS 2.2: Creating a Hierarchical GIIS, Available from: http://www.globus.org .

[10] Overview of Security-Enhanced Linux Type Enforcement and Role-Based Access Control Statements, Available from: http://www.tresys.com

[11] RBAC in the Solaris Operating Environment, Available from: http://www.sun.com

ภาคผนวก

ภาคผนวก ก
ผลงานตีพิมพ์

การประชุมทางวิชาการด้านเทคโนโลยีอินเทอร์เน็ต (The Conference on Internet Technology (CIT2003)) เมื่อวันที่ 12-13 พฤษภาคม 2546 ในบทความเรื่อง Access Control Service for Collective Information on Grid โดยผู้แต่งคือ Natthakrit Sanguandikul and Natawut Nupairoj

Access Control Service for Collective Information on Grid

ระบบการควบคุมการเรียกดูข้อมูลภายในกริด

Natthakrit Sanguandikul and Natawut Nupairoj

Department of Computer Engineering
Chulalongkorn University
ramza_th@yahoo.com, natawut.n@chula.ac.th

บทคัดย่อ. เทคโนโลยีกริดกำลังได้รับความสนใจอย่างแพร่หลายจากทั้งนักวิจัยและนักธุรกิจทั่วโลกเนื่องจากความสามารถในการรวบรวมเอาทรัพยากรมาใช้งานร่วมกันระหว่างองค์กรต่างๆ แต่เพราะในปัจจุบันกริดมักถูกนำไปใช้ในการประมวลผลที่ต้องการประสิทธิภาพการคำนวณเท่านั้น ยังขาดการศึกษาปัญหาของการควบคุมการเรียกดูข้อมูลของทรัพยากรที่ถูกแลกเปลี่ยนระหว่างเซิร์ฟเวอร์ภายในระบบกริด จึงทำให้เกิดแนวความคิดของการควบคุมการเรียกดูข้อมูลภายในกริดที่จะทำให้เจ้าของทรัพยากรสามารถควบคุมการสืบค้นข้อมูลไม่ว่าผู้ใช้งานคนนั้นๆจะเรียกดูข้อมูลจากเซิร์ฟเวอร์ใดภายในระบบกริดก็ตาม โดยบทความนี้จะอธิบายแนวคิดของระบบการควบคุมการเรียกดูข้อมูลภายในกริดทั้งด้านความสามารถพื้นฐานและองค์ประกอบที่สำคัญ และเราจะอธิบายขั้นตอนการพัฒนาแนวความคิดดังกล่าว ลงบนระบบโกลบัสซึ่งเป็นกริดซอร์ฟแวร์ที่มีการใช้งานอย่างแพร่หลายและอนุญาตให้ผู้ที่สนใจในระบบการทำงานแบบกริดนำไปทดลองติดตั้งและทำการศึกษาวิจัยโดยไม่คิดค่าใช้จ่ายแต่อย่างใด

1 บทนำ

จากแนวโน้มของการทำงานร่วมกันของธุรกิจในลักษณะองค์กรเสมือน (VO: Virtual Organization) ทำให้เทคโนโลยี กริด เข้ามามีบทบาททั้งในภาคการศึกษาและในภาคธุรกิจ ทั้งนี้เนื่องมาจากความสามารถของกริดในการควบคุมการใช้งานของทรัพยากรต่างๆของแต่ละองค์กรให้เป็นไปตามนโยบายที่ได้ถูกกำหนดขึ้นร่วมกัน ทำให้ทรัพยากรต่างๆเหล่านั้นเสมือนว่าอยู่รวมกันในลักษณะที่เรียกว่าทรัพยากรร่วม (Collective Resource) ซึ่งไม่ขึ้นกับสภาพของการเชื่อมต่อจริงภายในแต่ละองค์กร

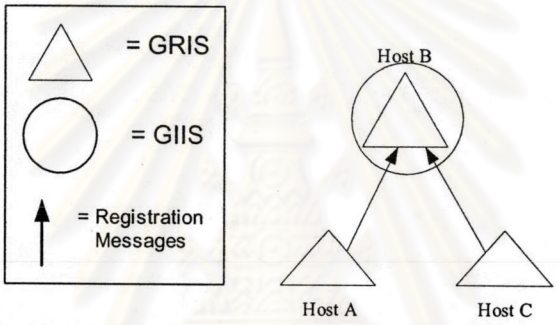
ระบบที่รองรับการทำงานแบบกริดที่ได้รับการยอมรับอย่างกว้างขวางในปัจจุบัน ได้แก่ ระบบโกลบัส (Globus) [1] โดยโกลบัสจะทำการควบคุมการใช้ทรัพยากรต่างๆโดยผ่านทางแกรม (GRAM: Grid Resource Allocation Management), ทำการจัดการข้อมูลของแต่ละทรัพยากรย่อยๆ ผ่านทางจีอาร์ไอเอส (GRIS : Grid Resource Information Service) และทำการเก็บรวบรวมข้อมูลทั้งหมดภายในแต่ละองค์กรเสมือนผ่านทางจีไอไอเอส (GIIS: Grid Institution Index Service) ซึ่งเป็นส่วนหนึ่งของระบบเอ็มดีเอส (MDS: Monitoring and Discovering Service) โดยระบบโกลบัสจะพิจารณาสิทธิการใช้งานของผู้ใช้จากชื่อเฉพาะของผู้ใช้แต่ละคน (DN: Distinguished Name) ว่าผู้ใช้มีรายชื่อเฉพาะอยู่ในทะเบียนเก็บอยู่ภายในเซิร์ฟเวอร์ที่เป็นทรัพยากร ซึ่งถ้ามีรายชื่อ จะยอมให้ผู้ใช้เข้าใช้งานทรัพยากรต่างๆได้

เนื่องจากการทำงานในลักษณะดังกล่าวจึงทำให้เกิดปัญหาในกรณีที่ที่เจ้าของทรัพยากรที่เป็นแหล่งกำเนิดข้อมูลภายในองค์กรเสมือนที่ถูกเรียกดูข้อมูลนั้น ไม่สามารถที่จะควบคุมสิทธิการให้ดูข้อมูลของตนในกรณีที่ข้อมูลดังกล่าวถูกคัดลอกไปเก็บไว้ยังเซิร์ฟเวอร์อื่น ซึ่งถึงแม้ว่าปัจจุบันได้มีงานวิจัยที่เกี่ยวข้องกับการควบคุมสิทธิสำหรับผู้ใช้งานภายใน กริดโดยไม่จำเป็นต้องไปกำหนดสิทธิการใช้งานของผู้ใช้งานแต่ละคนภายในแต่ละเครื่องเซิร์ฟเวอร์ย่อยๆแต่อย่างใด [2] แต่ทว่างานวิจัยดังกล่าวยังคงมุ่งเน้นแต่การควบคุมสิทธิของทรัพยากรต่างๆ โดยยังไม่ได้พิจารณาถึงปัญหาการขาดความสามารถในการควบคุมการเรียกดูของข้อมูลของเจ้าของทรัพยากรในกรณีที่ข้อมูลดังกล่าวถูกคัดลอกไปเก็บยังแต่ละจีไอไอเอส บนคนละเซิร์ฟเวอร์ แต่อย่างใด

จากปัญหาดังกล่าว ได้นำไปสู่แนวความคิดที่จะทำการออกแบบระบบการควบคุมการเรียกดูข้อมูลภายในกริดที่จะทำการเพิ่มเติมข้อมูลสิทธิการเข้าถึง เข้าไปรวมกับข้อมูลเดิมที่มาจากแต่ละทรัพยากรย่อยๆภายในองค์กรเสมือนนั้นๆ ซึ่งจะทำหน้าที่เป็นใบกำกับการเรียกใช้งานที่ระบบการควบคุมการเรียกดูข้อมูลภายในกริดจะนำไปพิจารณาเพื่อให้เจ้าของทรัพยากรสามารถควบคุมผู้ที่จะสามารถเรียกดูข้อมูลของตนไม่ว่าข้อมูลดังกล่าวนี้จะถูกคัดลอกไปยังเซิร์ฟเวอร์อื่นภายในระบบกริดอีกกี่ทอดก็ตาม โดยบทความจะมีโครงสร้างดังนี้ ในหัวข้อที่ 2 จะกล่าวถึงลักษณะของปัญหาที่เกิดขึ้นในการเรียกดูข้อมูลภายในกริดในปัจจุบัน ในหัวข้อที่ 3 จะอธิบายแนวคิดระบบการควบคุมการเรียกดูข้อมูลภายในกริดและองค์ประกอบที่สำคัญภายในระบบ ในหัวข้อที่ 4 จะอธิบายถึงขั้นตอนการพัฒนาระบบการควบคุมการเรียกดูข้อมูลภายใน กริดบนระบบโกลบัส และในหัวข้อที่ 5 จะเป็นการสรุปผลและงานวิจัยในอนาคต

2 ตัวอย่างของปัญหาที่เกิดขึ้นในปัจจุบัน

เนื่องจากในปัจจุบันโครงสร้างของระบบเอ็มดีเอสภายในระบบโกลบัสยังมีข้อจำกัดในแง่ของการควบคุมการเรียกดูข้อมูลเกี่ยวข้องของทรัพยากรของผู้ใช้แต่ละคนภายในองค์กรเสมือน โดยผู้ใช้จะสามารถเรียกดูข้อมูลทั้งหมดที่ถูกเก็บอยู่ในจีไอไอเอสภายในเซิร์ฟเวอร์นั้น ซึ่งเป็นส่วนที่เก็บรวบรวมข้อมูลจากแต่ละทรัพยากรย่อยๆภายในองค์กรเสมือนได้ โดยระบบโกลบัสจะทำการตรวจเพียงว่ามีชื่อเฉพาะของผู้ใช้ดังกล่าวภายในทะเบียนรายชื่อของเซิร์ฟเวอร์นั้นหรือไม่ ดังนั้น ในกรณีที่เจ้าของทรัพยากรได้ทำการส่งข้อมูลไปเก็บไปจีไอไอเอสซึ่งอยู่บนเซิร์ฟเวอร์อื่น เจ้าของทรัพยากรจะไม่สามารถควบคุมการเข้าถึงข้อมูลทรัพยากรของผู้ใช้ ดังรูปที่ 1

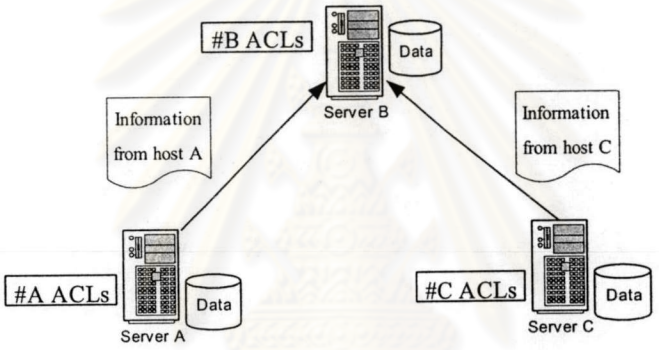


รูป. 1. การส่งข้อมูลของแต่ละเซิร์ฟเวอร์ย่อยภายในองค์กรเสมือนตัวอย่าง

จากรูปที่ 1 จะแสดงให้เห็นว่า ข้อมูลทั้งหมดที่ถูกเก็บอยู่ภายในจีอาร์ไอเอส ของแต่ละเซิร์ฟเวอร์ A, B และ C ตามลำดับจะถูกนำไปเก็บไว้ภายใน จีไอไอเอสภายในเซิร์ฟเวอร์ B เพราะฉะนั้นจึงจะทำให้ผู้ใช้งานที่ได้จดทะเบียนชื่อเฉพาะไว้กับเครื่อง B ที่เป็นเครื่องที่เก็บข้อมูลทั้งหมดภายในองค์กรเสมือนตัวอย่างนี้จะสามารถเห็นข้อมูลทั้งหมดภายในเครื่องเซิร์ฟเวอร์ทั้งเครื่อง A, B และ C ทั้งๆที่ ผู้ใช้คนนั้นไม่ได้เป็นสมาชิกของเครื่องเซิร์ฟเวอร์ A และ C แต่อย่างใด

ซึ่งถึงแม้ว่าในปัจจุบันได้มีงานวิจัยที่เกี่ยวกับการกำหนดการควบคุมการเข้าถึงของข้อมูลภายในโครงสร้างการแลกเปลี่ยนข้อมูลผ่านทางมาตรฐานแอลแด็ป (LDAP: Lightweight Directory Access Protocol) [3] โดยจะอาศัยการกำหนดเอ็กเซสคอนโทรลลิสท์ (ACL: Access Control Lists) [4] ซึ่งจะเป็นการอธิบายว่าใครบ้างที่สามารถจัดการข้อมูลที่ถูกเก็บอยู่ภายในแต่ละเซิร์ฟเวอร์ได้ ข้อมูลที่ใช้อธิบายลักษณะการควบคุมดังกล่าวจะถูกเก็บอยู่ภายในไฟล์ของเครื่องที่ให้บริการแอลแด็ปและจะถูกเรียกตอนเปิดแอลแด็ปเซิร์ฟเวอร์ ซึ่งลักษณะของการทำงานดังกล่าวจะทำให้เกิดปัญหาของการแยก

กันระหว่างตัวข้อมูลและสิทธิที่จะเป็นตัวอธิบายข้อมูลในกรณีที่มีการส่งข้อมูลดังกล่าวจากต้นตอของข้อมูลที่เก็บอยู่ใน จีอาร์ไอเอส (GRIS : Grid Resource Information Service) ไปยัง จีไอไอเอส (GIIS: Grid Institution Index Service) ซึ่งทำหน้าที่เก็บรวบรวมของมูลทั้งหมดของภายในองค์เสมือนซึ่งอยู่บนเซิร์ฟเวอร์อื่นดังในรูปที่ 2 เพราะสิ่งที่ถูกแลก เปลี่ยนระหว่างแต่ละเซิร์ฟเวอร์จะมีแต่ตัวข้อมูลเท่านั้นจึงจำเป็นให้ผู้ดูแลแต่ละเซิร์ฟเวอร์ต้องมาทำการกำหนดเอ็กเซสคอนโทรลลิสท์ ภายในแต่ละเซิร์ฟเวอร์ที่ตนรับผิดชอบเองเพื่อให้เป็นไปตามความต้องการของเจ้าของทรัพยากรของเซิร์ฟเวอร์อื่นอีกครั้งหนึ่ง จึงทำให้ยากแก่การควบคุมดูแลสิทธิการเข้าถึงข้อมูลในกรณีที่ข้อมูลภายในองค์เสมือนมีจำนวนเพิ่มมากขึ้น



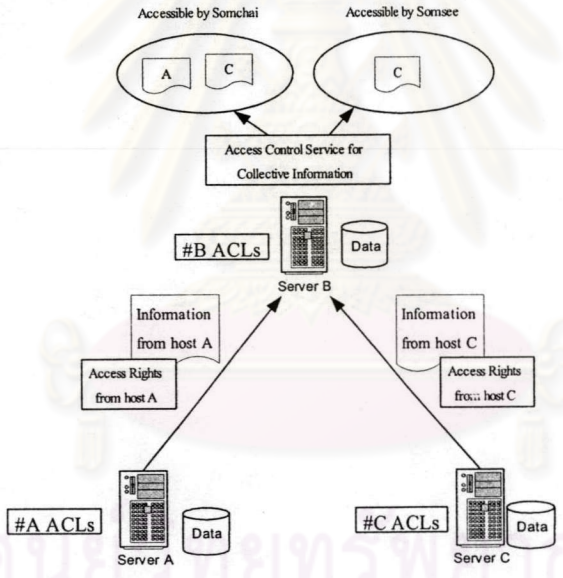
รูป. 2. ปัญหาของการแยกกันระหว่างตัวข้อมูลและเอ็กเซสคอนโทรลลิสท์ระหว่างแอลแค็ปเซิร์ฟเวอร์

จากตัวอย่างที่ได้ยกมาแสดงให้เห็นว่าในปัจจุบัน เมื่อมองในแง่ที่ว่าข้อมูลต่างๆที่ถูกเก็บอยู่ภายในแต่ละแอลแค็ปเซิร์ฟเวอร์ก็เป็นทรัพยากรอย่างหนึ่งเหมือนกัน ระบบโกลบัสยังขาดความสามารถในการควบคุมการเข้าถึงข้อมูลที่ตอบสนองต่อการทำงานในลักษณะองค์กรเสมือน ที่จะทำการรวบรวมเอาทรัพยากรต่างๆเข้าด้วยกันโดยยังรักษาสิทธิของเจ้าของทรัพยากรไว้ ซึ่งปัญหาดังกล่าวถึงแม้อาจจะไม่สำคัญในแง่ของการนำเอากริดเทคโนโลยีไปใช้เพื่อการศึกษาวิจัย แต่ปัญหานี้จะทวีความสำคัญขึ้นเมื่อเทคโนโลยีกริดถูกนำไปใช้ในโลกธุรกิจที่ข้อมูลข่าวสารต่างๆมีความสำคัญ

3 ระบบการควบคุมการเรียกดูข้อมูลภายในกริด

3.1 แนวความคิดพื้นฐาน

เนื่องจากปัญหาที่ได้กล่าวไว้ข้างต้น จึงได้นำไปสู่แนวความคิดของระบบการควบคุมการเรียกดูข้อมูลภายใน กริด (Access Control Service for Collective Information on Grid) ที่จะเปิดโอกาสให้ เจ้าของทรัพยากรที่เป็นแหล่งกำเนิดข้อมูลทรัพยากรภายในระบบกริด สามารถกำหนดผู้ที่มีสิทธิในการเรียกดูข้อมูลนั้นๆ โดยจะทำการกำหนดรูปแบบของข้อมูลสิทธิการเข้าถึง ที่จะอธิบายรายละเอียดเกี่ยวกับผู้ที่มีสิทธิและเครื่องเซิร์ฟเวอร์ที่สามารถดูข้อมูลดังกล่าวได้ ควบคู่ไปกับข้อมูลจริงที่จะส่งไปยังหน่วยที่เก็บรวบรวมข้อมูลภายในเซิร์ฟเวอร์อื่นที่ติดตั้งกริดซอร์ฟแวร์ เพื่อให้เจ้าของทรัพยากรสามารถวางใจได้ว่าข้อมูลของตนนั้นจะถูกจำกัดให้ถูกเรียกดูได้เฉพาะผู้ที่เจ้าของทรัพยากรยินยอมเท่านั้นไม่ว่าผู้ใช้ดังกล่าวจะเรียกดูจากบนเซิร์ฟเวอร์อะไรก็ตามดังรูปที่ 3



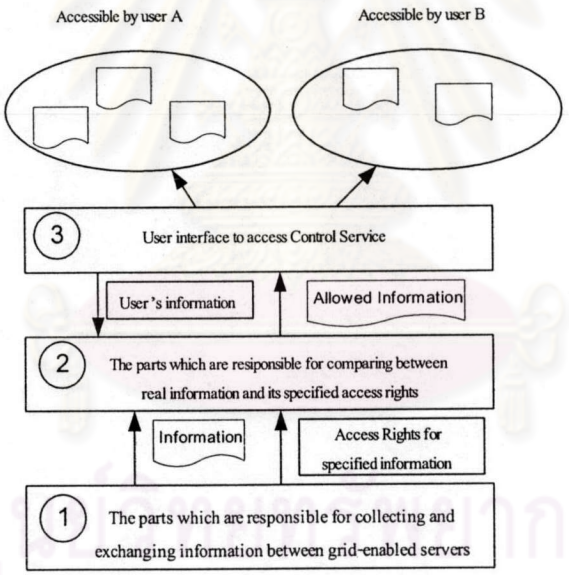
รูป. 3. การควบคุมสิทธิการเรียกใช้ข้อมูลโดยเจ้าของทรัพยากร
หลังการติดตั้งระบบควบคุมการเรียกดูข้อมูลภายในกริด

จากรูปตัวอย่างแสดงให้เห็นว่า เจ้าของทรัพยากรภายในเครื่อง A สามารถที่จะควบคุมให้เฉพาะนายสมชายเท่านั้นที่สามารถดูข้อมูลที่มาจากทรัพยากรของตนได้ และเจ้าของทรัพยากรในเครื่อง C ก็

สามารถกำหนดให้ทั้งนาย สมชายและนางสมศรีสามารถดูข้อมูลของตนได้ จึงทำให้ทั้งนาย สมชาย และนางสมศรีมองเห็นข้อมูลภายในองค์กรเสมือนแตกต่างกันตามความต้องการของเจ้าของทรัพยากรย่อยๆที่เป็นต้นตอของข้อมูลภายในระบบกริด ซึ่งเจ้าของข้อมูลจำเป็นที่จะต้องเพิ่มเติมข้อมูลสิทธิการเข้าถึงเข้าไปในข้อมูลที่ถูกแลกเปลี่ยนระหว่างเซิร์ฟเวอร์ภายในระบบกริดเพื่อให้ระบบการควบคุมการเรียกดูข้อมูลสามารถนำไปพิจารณาในกรณีที่มีผู้ใช้คนอื่นแสดงความประสงค์ที่จะของดูข้อมูลดังกล่าว

3.2 โครงสร้างของระบบการควบคุมการเรียกดูข้อมูลภายในกริด

เพื่อให้บรรลุวัตถุประสงค์หลักนอกจากการระบุข้อมูลสิทธิการเข้าถึงดังกล่าวแล้ว เรายังจำเป็นต้องกำหนดองค์ประกอบการควบคุมการเรียกดูข้อมูลภายในกริดโดยมุ่งเน้นที่การใช้ประโยชน์จากหน่วยให้บริการข้อมูลที่มีอยู่เดิม เช่น เอ็มดีเอสดังรูปที่ 4



รูป.4. โครงสร้างพื้นฐานของระบบการควบคุมการเรียกดูข้อมูล

- **ส่วนที่ 1 : ส่วนเก็บรวบรวมข้อมูลและส่วนที่ทำการแลกเปลี่ยนข้อมูลระหว่างแต่ละเซิร์ฟเวอร์** เพื่อความสะดวกเราอาจจะใช้ หน่วยให้บริการข้อมูล (Information Provider) ที่มีอยู่เดิมของกริดซอร์ฟแวร์ที่เราจะเพิ่มระบบการควบคุมการเรียกใช้ข้อมูลลงไป ซึ่งอาจจะอยู่ในรูปของดาต้าเบสชนิดต่างๆ โดยไม่จำเป็นที่จะต้องกำหนดมาตรฐานใหม่แต่อย่างใด ในกรณีของ ระบบโกลบัส เราจะใช้โครงสร้างของเอ็มดีเอสที่มีการเก็บข้อมูลพื้นฐานในรูปของฐานข้อมูลแอลแด็ปเก็บข้อมูลทั้งข้อมูลจริงภายในแต่ละองค์กรเสมือนและข้อมูลสิทธิการเข้าถึงที่เข้าของทรัพยากรได้เพิ่มเข้าไป ส่วนการแลกเปลี่ยนข้อมูลก็สามารถใช้ลักษณะการส่งข้อมูลที่มีอยู่เดิมได้เพราะเมื่อมองจากมุมมองของกริดแล้ว ข้อมูลสิทธิการเข้าถึงก็ไม่แตกต่างจากข้อมูลทั่วไปที่ถูกเพิ่มเข้าไปในกริด

- **ส่วนที่ 2 : ส่วนเปรียบเทียบข้อมูล** ซึ่งเป็นส่วนที่รับผิดชอบเกี่ยวกับการเปรียบเทียบระหว่างข้อมูลทั้งหมดที่เก็บอยู่ภายในระบบกริดเดิม กับข้อมูลสิทธิการเข้าถึงที่ถูกเพิ่มเข้าไปภายในระบบเพื่อกำกับลักษณะการถูกเรียกดูของข้อมูลดังกล่าว

- **ส่วนที่ 3 : ส่วนของโปรแกรมติดต่อของผู้ใช้งาน** จะเป็นระบบที่จะเปิดโอกาสให้ผู้ใช้งานสืบค้นข้อมูลที่ตนต้องการจากข้อมูลทั้งหมดภายในองค์กรเสมือน ซึ่งจะเป็นคนนำเอาข้อมูลทั้งหมดที่ผู้ใช้ร้องขอ พร้อมกับรายละเอียดของผู้ร้องขอส่งไปยังส่วนเปรียบเทียบข้อมูลเพื่อให้ได้ผลลัพท์กลับคืนมาเฉพาะข้อมูลที่ผู้ใช้คนนั้นมีสิทธิในการเรียกดูเท่านั้น

3.3 ชนิดของข้อมูลสิทธิการเข้าถึงที่จะถูกเพิ่มเข้าไปภายในระบบควบคุมการเรียกดูข้อมูลภายในกริด

เนื่องจากการวิจัยชิ้นนี้เป็นเพียงความพยายามที่จะเพิ่มความสามารถในการควบคุมการเรียกดูข้อมูลภายในระบบกริดเท่านั้น ข้อมูลสิทธิการเข้าถึงที่เลือกมาใช้จึงยังเป็นเพียงตัวอย่างซึ่งยังไม่ได้เป็นมาตรฐานแต่ประการใด โดยหัวข้อต่างๆของข้อมูลสิทธิการเข้าถึงที่จะถูกแนบไปกับข้อมูลจริงจะสามารถแบ่งออกได้เป็นหัวข้อต่างๆดังต่อไปนี้

- **ส่วนที่ใช้ในการระบุชื่อของผู้ที่สามารถเรียกข้อมูลได้หรือไม่ได้ของข้อมูล** โดยอาจจะระบุเป็นชื่อเฉพาะของผู้ใช้งานแต่ละคน (DN: Distinguished Name) หรืออาจจะใช้การประกาศโดยการอาศัยสัญลักษณ์พิเศษดังเช่นการใช้สัญลักษณ์ไวลด์คาร์ดเป็นต้น(เช่น /O=Grid/O=Globus/OU=zeus.cp.eng.chula.ac.th / CN=*)

- **ส่วนที่ใช้ในการอธิบายเครื่องเซิร์ฟเวอร์หรือกลุ่มของเซิร์ฟเวอร์** ซึ่งอาจจะใช้การอธิบายในรูปแบบของการใช้สัญลักษณ์พิเศษดังที่ใช้กับการระบุชื่อเครื่อง หรืออาจจะใช้ชื่อขององค์กรเสมือนในกรณีที่ภายในแต่ละองค์กรมีการแลกเปลี่ยนข้อมูลระหว่างองค์กรเสมือนมากกว่าหนึ่ง

- **ส่วนที่ใช้ในการอธิบายชนิดของข้อมูล** ซึ่งชื่อที่จะใช้ในการแบ่งหมวดหมู่ดังกล่าวจำเป็นจะต้องเป็นชื่อที่ทุกฝ่ายภายในองค์กรเข้าใจเหมือนกัน ดังเช่น หมวดหมู่ของข้อมูลที่เกี่ยวกับหน่วยประมวลผลเป็นต้น เพื่อให้ง่ายต่อการนำไปจัดแบ่งหมวดหมู่เพื่อให้ง่ายต่อการสืบค้น

4.รูปแบบการพัฒนาระบบการควบคุมการเรียกดูข้อมูลภายในกริดบนระบบโกลบัส

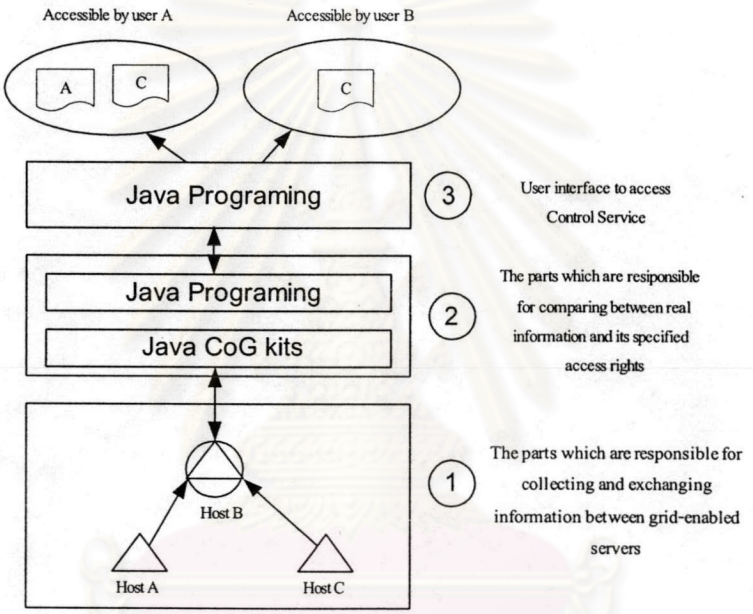
เราได้เลือกใช้ภาษาจาวาในการพัฒนาระบบที่นำเสนอ ทั้งนี้เพราะในปัจจุบันได้มีโครงงานวิจัยที่ได้พัฒนา คำสั่งพื้นฐานที่สามารถเรียกใช้เซอร์วิสต่างๆภายในกริดด้วยภาษาจาวา (Java CoGkits API) ซึ่งจะทำให้ไม่จำเป็นต้องไปแก้ไขโปรแกรมดิบ (Source Code) ของ โกลบัสทูลคิต ที่เป็นภาษาซี แต่อย่างใด

โครงสร้างของระบบการควบคุมการเรียกดูข้อมูลภายในกริดซึ่งเราได้เลือกทำการพัฒนาบนกริดซอร์ฟแวร์ โกลบัสทูลคิต รุ่น2.0 (Globus Toolkits 2.0) โดยจะทำการเพิ่มฟังก์ชั่นการควบคุมให้แก่เอ็มดีเอส โดยอาศัยการทำงานดั่งเดิมของเอ็มดีเอสเป็นพื้นฐาน และยังคงมาตรฐานของการติดต่อแลกเปลี่ยนข้อมูลระหว่างเซิร์ฟเวอร์ของเอ็มดีเอสเอาไว้ ดังรูปที่ 5

ซึ่งจากรูปจะสังเกตได้ว่าเราจะมีการเพิ่มเติมข้อมูลสิทธิการเข้าถึงที่มาจากเจ้าของทรัพยากรแต่ละคน นำไปเก็บอยู่ภายในจีไอไอเอสเดิมร่วมกับข้อมูลจริง เพื่อที่จะทำให้ข้อมูลสิทธิการเข้าถึงดังกล่าวจะถูกส่งไปยังเซิร์ฟเวอร์ใดๆควบคู่ไปกับข้อมูลจริงเสมอในกรณีที่ข้อมูลจริงดังกล่าวถูกคัดลอกไปเก็บไว้ยังเซิร์ฟเวอร์ตัวอื่น จึงทำให้ไม่จำเป็นต้องไปแก้ไปลักษณะของการแลกเปลี่ยนข้อมูลเดิมแต่อย่างใดเพียงแต่เป็นเพียงการเพิ่มข้อมูลเข้าไปในต้นไม้ข้อมูลภายในฐานข้อมูลแอลแด็ปเท่านั้น

เนื่องจากระบบโกลบัสจะเปิดโอกาสให้เราสามารถกำหนดโครงสร้างของข้อมูลภายในจีไอไอเอสได้อย่างอิสระเราจึงทำการเพิ่มเติมข้อมูลสิทธิการเข้าถึงทั้งหมดที่จำเป็นซึ่งเราได้กล่าวไว้ในหัวข้อ 3.3 จะถูกรวบรวมอยู่ในโหนดๆ หนึ่งจึงจะไปเป็นโหนดลูกของข้อมูลใดๆที่เราต้องการควบคุมซึ่งได้ถูกส่งมาพร้อมกับข้อมูลจริงโดยเจ้าของทรัพยากรที่เป็นต้นตอของข้อมูล ดังโครงสร้างของการเก็บข้อมูล

ภายในต้นไม้ข้อมูลของมาตรฐานแอลเด็ปภายใน จีไอไอเอสของเซิร์ฟเวอร์ B ซึ่งจะมีลักษณะดังรูปที่ 6 ที่เราจะสามารถควบคุมให้เฉพาะโหนด dn=memory, hn=apolo11.cp.eng.chula.ac.th, o=grid และโหนดลูกทั้งหมดเป็นข้อมูลประเภทประมวลผล (Computing Category) ซึ่งจะถูกดูได้โดย ผู้ใช้งานที่มีชื่อเฉพาะ (DN: Distinguished Name) คือ O=Grid/O=Globus/OU=zeus.cp.eng.chula.ac.th/CN=somchai เป็นต้น ซึ่งจะตรงกับตัวอย่างในหัวข้อ 3.1 ที่นายสมชายจะสามารถมองเห็นข้อมูลที่มาจากเซิร์ฟเวอร์ A ในขณะที่นางสมศรีไม่สามารถที่จะเรียกดูข้อมูลดังกล่าวได้

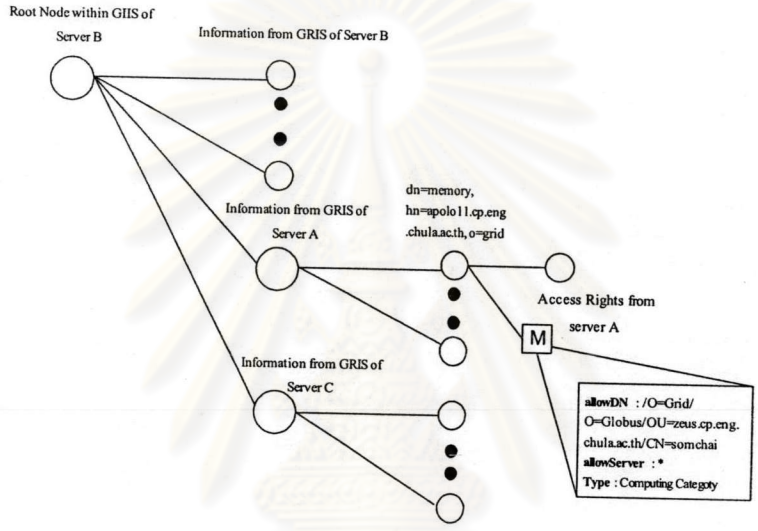


รูป. 5. โครงสร้างของระบบการควบคุมการเรียกดูข้อมูลบนกริด หลังจากพัฒนาบนระบบโกลบัส

5 สรุปผลและงานวิจัยในอนาคต

จากที่ได้แสดงให้เห็นในหัวข้อต่างๆที่ผ่านมาว่าเราสามารถที่จะเพิ่มเติมความสามารถในการควบคุมการเรียกดูข้อมูลโดยการเพิ่มข้อมูลสิทธิการเข้าถึงเข้าไปในโครงสร้างข้อมูลเดิม ซึ่งจะถูกส่งควบคู่ไปกับข้อมูลจริงภายในระบบกริดเพื่อให้เจ้าของทรัพยากรที่เป็นต้นตอของข้อมูลสามารถที่จะควบคุม

ลักษณะของผู้ที่มีสิทธิในการเรียกดูข้อมูลของตนได้ ซึ่งแนวความคิดดังกล่าวสามารถที่จะใช้โครงสร้างมาตรฐานของการเก็บและส่งข้อมูลเดิมภายในระบบกริดที่ใช้อยู่ในปัจจุบันจึงไม่จำเป็นต้องแก้ไขหรือพัฒนามาตรฐานใหม่มาใช้แทนแต่ประการใด ดังที่ได้แสดงให้เห็นในการพัฒนาแนวความคิดลงบนระบบโกลบัสโดยอาศัยเอ็มดีเอสซึ่งเป็นหน่วยให้บริการข้อมูลที่มีอยู่เดิมของระบบโกลบัสเป็นต้น



รูป. 6. โครงสร้างของข้อมูลภายในจีไอไอเอส
ภายหลังจากการติดตั้งระบบควบคุมการเรียกดูข้อมูลบนกริด

นอกจากความสามารถที่เราได้กล่าวไว้แล้วข้างต้น ในอนาคตเรายังจะสามารถประยุกต์หลักการของระบบควบคุมการเข้าถึงข้อมูล ไปใช้ในการเพิ่มประสิทธิภาพในด้านอื่นๆ ดังที่เช่นนำเอาหลักการของ การควบคุมสิทธิผ่านทางบทบาท (RBAC: Role-based Access Control) [5] มาใช้ภายในระบบเพื่อให้ง่ายต่อการควบคุมดูแลและการกำหนดสิทธิของผู้ใช้งานแต่ละคนเพราะบทบาทต่างๆที่นำเอามาพิจารณามักจะตรงกับบทบาทต่างๆที่ถูกกำหนดอยู่ในโครงสร้างการบริหารของแต่ละองค์กรอยู่แล้ว จึงทำให้ผู้ดูแลระบบทุกคนจะเห็นภาพของผู้ขอเรียกดูข้อมูลเหมือนกัน หรือนำเอาหลักการสร้างภาพข้อมูลเสมือนของผู้ใช้แต่ละคน ที่จะทำการแสดงข้อมูลที่ผู้ใช้แต่ละคนต้องการจากข้อมูลทั้งหมดที่ถูกเก็บอยู่ภายในองค์กรเสมือนตราบเท่าที่ยังอยู่ในขอบเขตสิทธิของผู้ใช้คนนั้น โดยที่ผู้ใช้แต่ละคนไม่จำเป็นที่จะต้องสืบค้นข้อมูลที่ตนต้องจากข้อมูลทั้งหมดภายในแต่ละองค์กรเสมือนด้วยตนเองแต่

ประการใด ซึ่งจำเป็นจะต้องนำเอาหลักการของการเพิ่มรายละเอียดของผู้ใช้แต่ละคน (User Profile) [6] จากเดิมที่ กริดจะมองเห็นผู้ใช้แต่ละคนจากชื่อเฉพาะ (DN: Distinguished Name) เท่านั้น นอกจากนี้ในปัจจุบันได้มีผู้ผลิตกริดซอร์ฟแวร์ชนิดอื่นๆนอกเหนือจากระบบโกลบัสที่กำลังจะเปิดตัวสู่ตลาดในอนาคต จึงทำให้มีความสนใจที่จะทำการศึกษาโครงสร้างการเก็บข้อมูลและการแลกเปลี่ยนข้อมูลของกริดซอร์ฟแวร์ชนิดอื่นๆดังเช่น SUN grid เพื่อศึกษาว่าเราจำเป็นต้องเพิ่มเติมหรือแก้ไขโครงสร้างของระบบการเรียกดูข้อมูลภายในกริด อย่างไรเพื่อให้ระบบควบคุมการเรียกดูข้อมูลภายในกริดสามารถทำงานได้โดยไม่ขึ้นกับชนิดของกริดซอร์ฟแวร์ต่อไป

รายการอ้างอิง

1 Foster, I., Kesselman, C., and Tuecke, S.: Anatomy of the Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications 15(3) (2001)

2 Pearlman, L., Welch, V., Foster, I., and Kesselman, C.: A Community Authorization Service for Group Collaboration

3 Wahl, M., Howes, T., and Kille, S.: RFC 2251 Lightweight directory access protocol (v3) (1997)

4 Brief Comments On LDAP ACLs (Access Control Lists): http://www.usenix.org

5 Sandhu, S., Coyne, J., Feinstein, L., and Youman, E.: Role-Base Access Control Models. 9th IEEE Computer Security Foundation Workshop Dromquinna Manor, Kenmare, County Kerry, Ireland, (1996) 38-47

6 Amato, G., and Straccia, U.: User Profile Modeling and Application to Digital Libraries: Italy: Istituto di Elaborazione dell'Informazione (2000)

ประวัติผู้เขียนวิทยานิพนธ์

นายณัฏฐกฤตย์ สงวนดีกุล สำเร็จการศึกษาหลักสูตรวิศวกรรมศาสตรบัณฑิต มหาวิทยาลัยจุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2544 และเข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2545